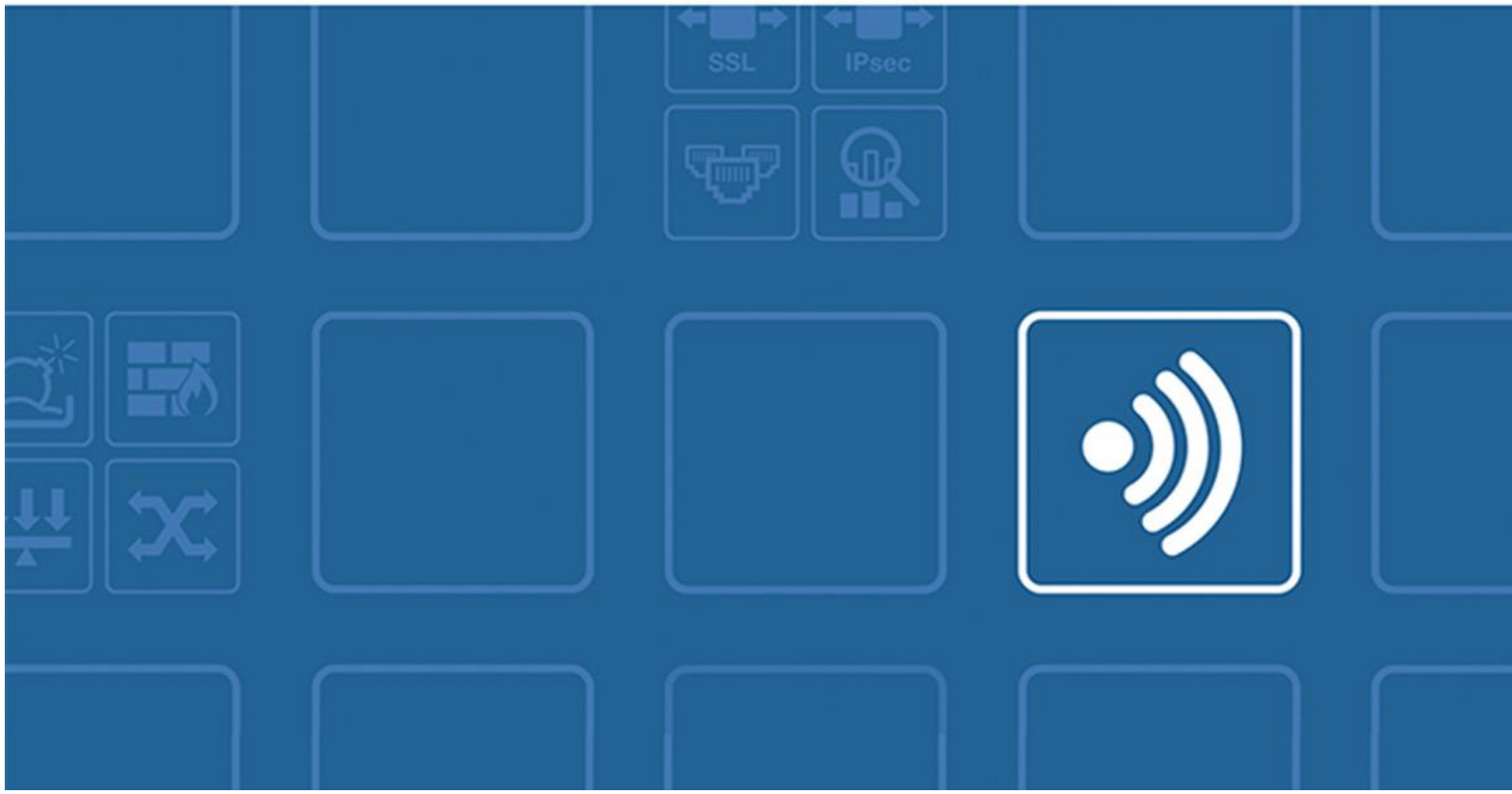
FORTINET
High Performance Network Security

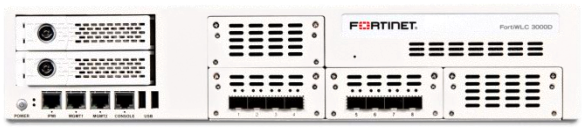
# FortiWLC (SD)

## Release 8.3.0



FortiWLC-SD 8.3.0 introduces two new controllers, the FortiWLC-1000D and FortiWLC-3000D to support large scale deployments.

## Fortinet Wireless LAN Controllers

| FortiWLC-1000D | FortiWLC-3000D |
|---|---|
|  |  |

Additionally, this release also introduces features and enhancements as listed under the new features section.

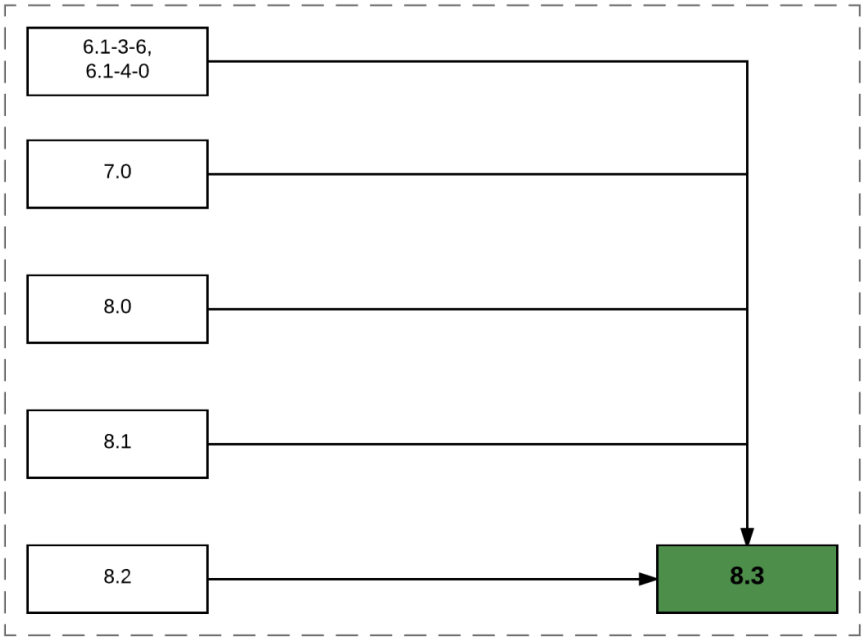
To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

# Getting Started with Upgrade

The following are important points to note before you begin installaing or upgrading to this release.

- The new FortiWLC controllers (1000D and 3000D) must be upgraded to the latest GA release before proceeding with any configuration steps..
- In a large-scale deployment with 1000D or 3000D, we recommend that you upgrade APs in batches.
- When deploying 1000D or 3000D, ensure that a subnet has only one controller. To use more than one controller per subnet, we recommend that you map different VLANs ESS profiles across controllers or within controllers.
- Disable *New APs Join ESS* option on all ESS profile if your network requires 64 ESS profiles per AP
- Open CAPWAP ports 5246 and 5247 in firewall before deploying/upgrading to 8.3.0
- Read the Upgrade Advisories, and Known Issues and Limitations sections before you begin installing or upgrading.

The following flowchart illustrates the approved upgrade path applicable for all controllers except FortiWLC-1000D and FortiWLC-3000D. The new controllers require a fresh installation. See the Installing 8.3 on FortiWLC-1000D and a FortiWLC-3000D section for specific instructions.




## Supported Upgrade Releases

| Release | GoTo Release Numbers |
|---|---|
| 6.1 | 6.1.3-6, 6.1.4-0 |
| 7.0 | 7.0-1-0, 7.0-2-0, 7.0-3-1, 7.0-4-0. 7.0-9-1,7.0-10-0 |
| 8.0 | 8.0-5-0, 8.0-6-0 |
| 8.1 | 8.1-2-0, 8.1-3-0 |
| 8.2 | 8.2.4 |

Controller upgrade performed via CLI interface will require a serial or SSH2 connection to connect to the controller and use its CLI.

## Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **`show file systems`** command to verify the current disk usage.

```
controller# show file systems
Filesystem 1K-blocks Used   Available Use% Mounted on
/dev/hdc2  428972    227844 178242    57%  /
none       4880      56     4824      2%   /dev/shm
…
```

The first partition (in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **`delete flash:<flash>`** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the currently running version).

## Set up Serial Connection

Set the serial connection for the following options:

- Only one terminal session is supported at a time. Making multiple serial connections causes signaling conflicts, resulting in damage or loss of data.
- Commands in SSH connection cannot contain ‘ **;**’ (semi-colon) and ‘**&**’ (ampersand) characters.

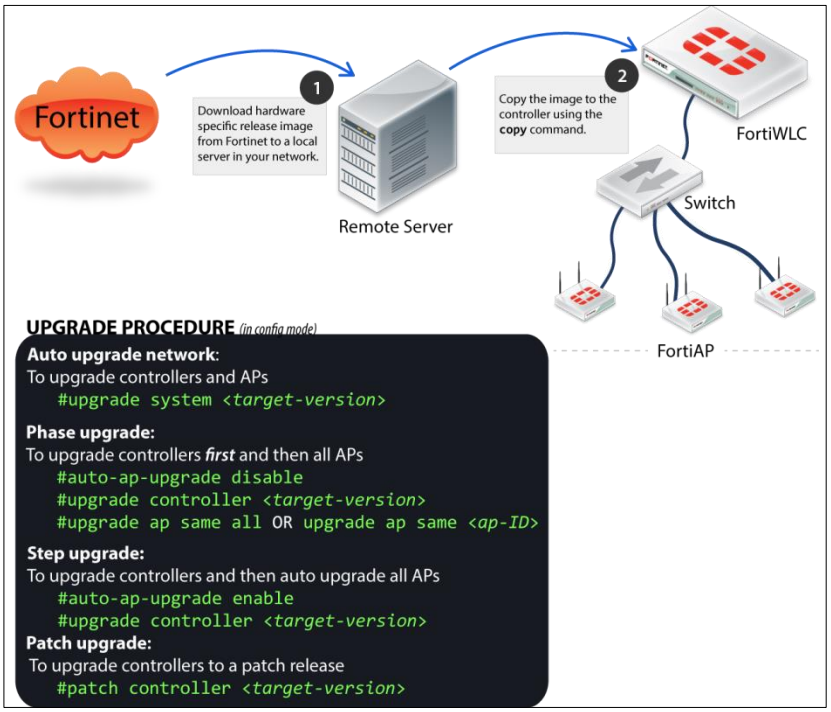
- Baud--115200
- Data--8 bits
- Parity--None
- Stop Bit—1
- Flow Control—None

## Supported Hardware and Software

| Hardware and Software | Supported | | Unsupported |
|---|---|---|---|
| Access Points | AP122<br>AP822e, AP822<br>AP832e, AP832i, OAP832e<br>AP332e, AP332i*<br>AP433e, AP433i,<br>OAP433e*<br>FAP U421EV<br>FAP U423EV | AP1010e, AP1010i*<br>AP1020e, AP1020i*<br>AP1014i*<br>AP110*<br>AP822<br>PSM3x* | AP300, AP301, AP302,<br>AP302i, AP301i<br>AP310, AP311, AP320,<br>AP310i, AP320i |
| *Cannot be configured as a relay AP | | | |
| Controllers | FortiWLC 50D<br>FortiWLC 200D<br>FortiWLC 500D<br>FortiWLC 1000D#<br>FortiWLC 3000D#<br>MC6000<br>MC4200 (with or without 10G Module)<br>MC4200-VE<br>MC3200, MC3200-VE<br>MC1550, MC1550-VE | | MC 1500<br>MC 1500-VE<br>#Spectrum Manager NOT supported in FWLC-1000D and FWLC-3000D |
| FortiWLM | 8.3.0 | | |
| FortiConnect | 16.7 | | |
| **Browsers** | | | |
| FortiWLC (SD) WebUI | Internet Explorer 9,10<br>Mozilla Firefox 25+<br>Google Chrome 31+ | | |
| A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs. | | | |
| Captive Portal | Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge.<br>Apple Safari<br>Google Chrome<br>Mozilla Firefox 4.x and earlier<br>Mobile devices (such as Apple iPhone and BlackBerry) | | |

# Installing and Upgrading

- The following instructions apply to all controllers except 1000D and 3000D. See the Installing 8.3 on FortiWLC-1000D and a FortiWLC-3000D section for specific instructions.




1. Download image files from the remote server to the controller using one of the following commands:

```
# copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar><space>.
[OR] # copy tftp://<ext-ip-addr>/<image-name-rpm.tar><space>.
```

   - **image-name** for legacy controllers: meru-{***release-version***}-{***hardware-model***}-rpm.tar. Eg,: meru-***8.3-0-MC4200***-rpm.tar
   - **image-name** for FortiWLC: forti-{***release-version***}-{***hardware-model***}-rpm.tar. Eg,: forti-***8.3-0-FWC2HD***-rpm.tar
2. Disable AP auto upgrade and then upgrade the controller (in config mode)

```
# auto-ap-upgrade disable
# copy running-config startup-config
# upgrade controller <target version> (Example, upgrade controller 8.3)
```

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the `show controller` and `show ap` command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the `show running-config` command (if not, recover from the remote location). See the Backup Running Configuration step.

# Installing on FortiWLC-1000D and FortiWLC-3000D

To install release 8.3.0 on the new controllers, use the following instructions:

The new controllers have two logical partitions, and the default image is available in both the partitions.

## Upgrading via CLI

1. Use the `show images` command to view the available images in the controller. By default, a new controller will boot from the primary partition which contains the running image.

```
default(15)# sh images
Running image: Primary ← denotes current partition
--------------------------------------------------------------------------------
Running image details.
         System version: 0.0.7
         System hash: e9efe2c7ab0d10da660cad019d333f8d7772d6f1
         System branch: master
         System built: 20161115072723
         System memory: 114M/463M ←Shows available/total memory.
         Apps version: 8.3-0build-46
         Apps size: 303M/850M
--------------------------------------------------------------------------------
Other image details.
         System version: 0.0.7
         System hash: e9efe2c7ab0d10da660cad019d333f8d7772d6f1
         System branch: master
         System built: 20161115072723
         System memory: 150M/473M
         Apps version: False
         Apps size: 662M/849M
```

2. To install the latest release, download the release image using the ***upgrade-image*** command:

```
upgrade-image scp://<username>@<remote-server-ip>:<path-to-image>/<image-name>-rpm.tar both reboot
```

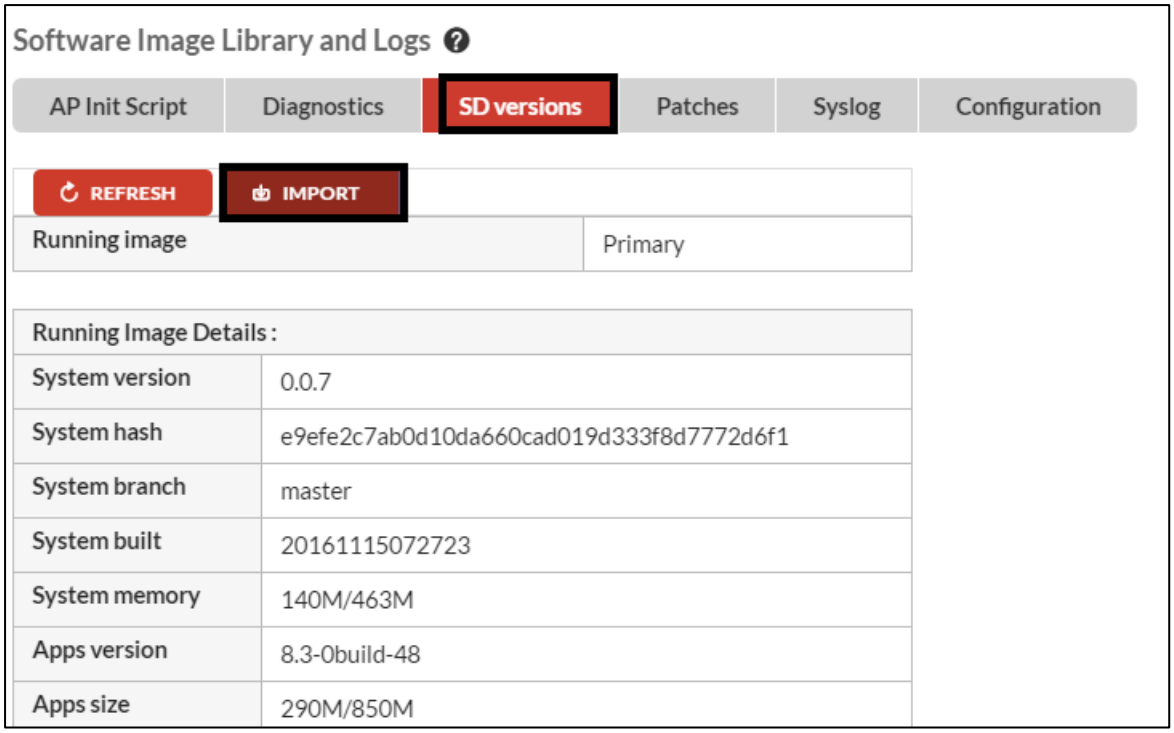
The above command will upgrade the secondary partition and the controller will reboot to secondary partition. The option **both** upgrades the system files and apps files.

After an upgrade the current partition will shift to the second partition. For example, if you started upgrade in primary partition, post upgrade the default partition becomes secondary partition and vice-versa.

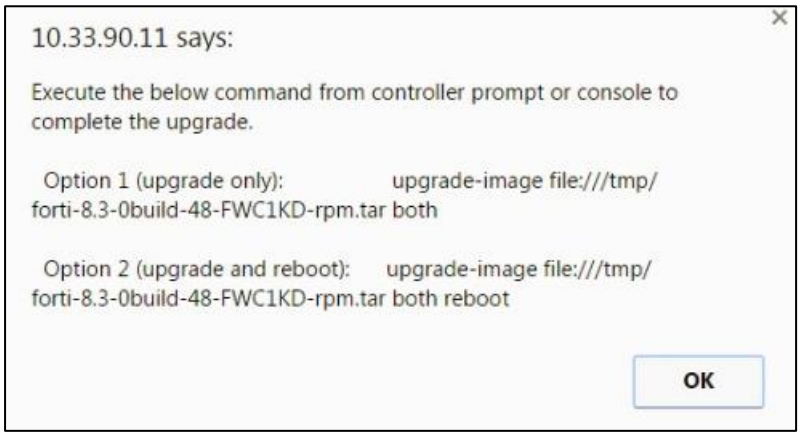
```
default(15)# sh images
Running image: Secondary ← Current partition after the upgrade.
--------------------------------------------------------------------------------
Running image details.
         System version: 0.0.7
         System hash: e9efe2c7ab0d10da660cad019d333f8d7772d6f1
         System branch: master
         System built: 20161115072723
         System memory: 150M/473M
         Apps version: 8.3-0build-47
         Apps size: 230M/849M
--------------------------------------------------------------------------------
Other image details.
         System version: 0.0.7
         System hash: e9efe2c7ab0d10da660cad019d333f8d7772d6f1
         System branch: master
         System built: 20161115072723
         System memory: 116M/463M
         Apps version: 8.3-0build-46
         Apps size: 298M/850M
```

## Upgrading via WebUI

1. To upgrade controllers using FortiWLC-SD WebUI, navigate to **Maintenance** > **File Management** > **SD Version**.
2. Click **Import** button to choose the image file.




3. After the import is complete, the following message is displayed.




4. Now, from the CLI run the upgrade commands to complete the upgrade process.

### Switching Partitions

To switch partitions in FortiWLC-1000D and FortiWLC-3000D, select the partition (from the GRUB menu) during the bootup process. (***Ref***: *https://en.wikipedia.org/wiki/GNU_GRUB*)

## Upgrading a N+1 Site

To upgrade a site running N+1, all controllers must be on the same FortiWLC-SD version, and the backup controller must be in the same subnet as the primary controllers. You can choose any of the following options to upgrade.

**Option 1** - Just like you would upgrade any controller, you can upgrade a N+1 controller.

1. Upgrade master and then upgrade slave.
2. After the upgrade, enable master on slave using the `nplus1 enable` command.

**Option 2** - Upgrade slave and then upgrade master.

After the upgrade, enable master service on slave using the `nplus1 enable` command.

**Option 3** - If there are multiple master controllers

1. Upgrade all master controllers followed by slave controllers. After the upgrade, enable all master controllers on slave controllers using the `nplus1 enable` command.
2. To enable master controller on slave controller, use the `nplus1 enable` command.
3. Connect to all controllers using SSH or a serial cable.
4. Use the `show nplus1` command to verify if the slave and master controllers are in the cluster. The output should display the following information:

```
Admin: Enable
Switch: Yes
Reason: -
SW Version: 8.3.0
```

5. If the configuration does not display the above settings, use the `nplus1 enable <master-controller-ip>` command to complete the configuration.
6. To add any missing master controller to the cluster, use the `nplus1 add master` command.

## Restore Saved Configuration

1. Copy the backup configuration back to the controller:

```
# copy ftp://<user>:<passswd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
```

2. Copy the saved configuration file to the running configuration file:

```
# copy orig-config.txt running-config
```

3. Save the running configuration to the start-up configuration:

```
# copy running-config startup-config
```

## SFP Transceivers Supported for FortiWLC-1000D and FortiWLC-3000D

This table lists the SFP transceivers supported for the FortiWLC-1000D and FortiWLC-3000D.

| Supplier | Type | Part Numbers | Supported in FortiWLC-1000D | Supported in FortiWLC -3000D |
|---|---|---|---|---|
| Intel | DUAL RATE 1G/10G SFP+ SR (bailed) | FTLX8571D3BCV-IT | **Yes** | **Yes** |
| Finisar | SFP+ SR bailed, 10g single rate | FTLX8571D3BCL | **Yes** | **Yes** |

| | | | | |
|---|---|---|---|---|
| Avago | 10GBASE-SR/SW, SFP+ | AFBR-709ASMZ | **Yes** | **Yes** |
| Finisar | DUAL RATE 1G/10G SFP+ | FTLX8571D3BCV | **Yes** | **Yes** |
| HP | 1000BASE-SX SFP | SFP SX J4858C | **Yes** | **No** |
| Finisar | SFP+ SR, 10g single rate | FTLX 8574D3BCL | **Yes** | **Yes** |
| Axcen | SFP, 1000SX | AXGE-5854-0511 | **Yes** | **No** |
| Axcen | SFP, 1000SX | AX16020001566 | **Yes** | **No** |
| Dlink | 1GB Copper | DGS712 | **Yes** | **No** |
| AVAGO | 1GB Fiber | AFBR-5710PZ | **Yes** | **No** |
| Fiberxon 1 | 1GB Fiber | FTM-8012C-SL | **Yes** | **No** |
| Fiberxon 2 | 1GB Fiber | FTM-8012-SLG | **Yes** | **No** |
| Agilent | 1GB Fiber | HFBR 5710L | **Yes** | **No** |
| Picolight | 1GB Fiber | PL-XPL-VC-S13-11 | **Yes** | **No** |
| JDSU | 10GB Fiber | PLRXPL-SC-S43-22-N | **Yes** | **Yes** |
| AXCEN | 10GB Fiber | AXXE-5886-05B1 | **Yes** | **Yes** |
| Finisar | 1GB Copper | FCLF-8521-3 | **Yes** | **Yes** |
| Finisar | 1GB Copper | FCLF-8521P2BTL | **Yes** | **Yes** |
| Avago | Dual Rate 10GBASE-SR/1000BASE-SX | AFBR-709DMZ | **No** | **Yes** |
| Finisar | DUAL RATE 1G/10G SFP+ | FTLX8574D3BCVxxx | **No** | **Yes** |

# Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

## Devices with Intel Chipset

Wireless devices with Intel chipset must upgrade its firmware to version 19.x.x.

# Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller.

### Feature Groups in Mesh profile

If APs that are part of a mesh profile are to be added to feature group, all APs of that mesh profile should be added to the same feature group. Enable the *Override Group Settings* option in the ***Wireless Interface*** section in the Configuration > Wireless > Radio page on the gateway AP.

# Captive Portal and Fortinet Connect Deployment Recommendations

### DNS Entry

It is mandatory to enter the DNS while creating internal DHCP profile.

### External Portal IP Configuration:

If a NAT device is located between the controller and the Fortinet Connect, the IP address with which Fortinet Connect sees the controller should be configured under Device > RADIUS Clients page in Fortinet Connect Admin portal (*http://<fortinetconnect-ip-address>/admin*), . Select the RADIUS client and enter the controller IP address in the Client tab. The Fortinet Connect Automatic Setup then configures the controller correctly and ensures that the correct controller IP address is configured on Fortinet Connect.

### Remember Me settings

In the Portal Settings step of the Guest Portal configuration wizard, if you choose to enable Remember Credentials, then select "Initially attempt to use a cookie, if this fails try the MAC address" option. This removes the dependency on the client's browser and security settings.

### SmartConnect Certificate download

In the Certificates step of the Smart Connect Profile Wizard, ensure that you select the complete certificate chain of your uploaded certificate. If you have uploaded all certificates in the chain (from root to server), then selecting the server certificate will automatically select the entire certificate chain.

- To upload the server certificates, goto **Server** > **SSL Settings** > **Server Certificate** tab.
- To upload rest of the chain, goto **Server** > **SSL Settings** > **Trusted CA Certificates** tab.

# CNA Bypass for Android 5.0 +

Devices running Android 5.0 and above introduces system default CP login pop-up windows. To disable this pop-up window enable CNA bypass in the controller.

### In the WebUI

Go to **Configuration** > **Security** > **Captive Portal** > Advanced Settings section, select Captive Portal Prole and set **Apple Captive Network Assistant (CNA) Bypass** to **ON**.

### Using CLI

Use the **`ssl-server cna-bypass ON`** command in config mode.

## Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration** > **Devices** > **System Settings** > **Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and these results in a noticeable reduction of throughput in data traffic.

## IP Prefix Validation

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. A new field, IP Prefix Validation is added to the ***ESS Profile*** and ***Port Profile*** configuration page. When enabled, stations with different subnet are prevented from connecting to the controller. By default, IP Prefix Validation in **ESS Profile is ON** and in **Port Profile it is OFF**.

IP Prefix Validation must be disabled if the ESS profile is used for RAC.

## QoS Rules

QoS rules with no matching criteria when *Match* is checked will abort an upgrade. To prevent this, check QoS rules to ensure that at least one matching criteria is set for each rule if *Match* is set.

# Downgrade Procedure

Any controller that has been upgraded to 8.3 can only be downgraded to the previous release from which it was originally upgraded.

Obtain a signed image file for a downgrade from the FTP site and install it on the controller before the downgrading. To downgrade to an earlier release, use the upgrade procedure. Before downgrading to any release, save your configuration to a backup file and store it on a server accessible by FTP. The saved configuration can then be used to restore your configured parameters if needed. There are two upgrade command options.

You can upgrade the controller first using the **`upgrade controller`** command and then upgrade APs using the **`upgrade ap same all`** command. You can also use the **`upgrade system`** command; this downgrades the APs first, then the controller.

After downgrading, re-plan is required if ARRP is enabled in 8.3

# New Features

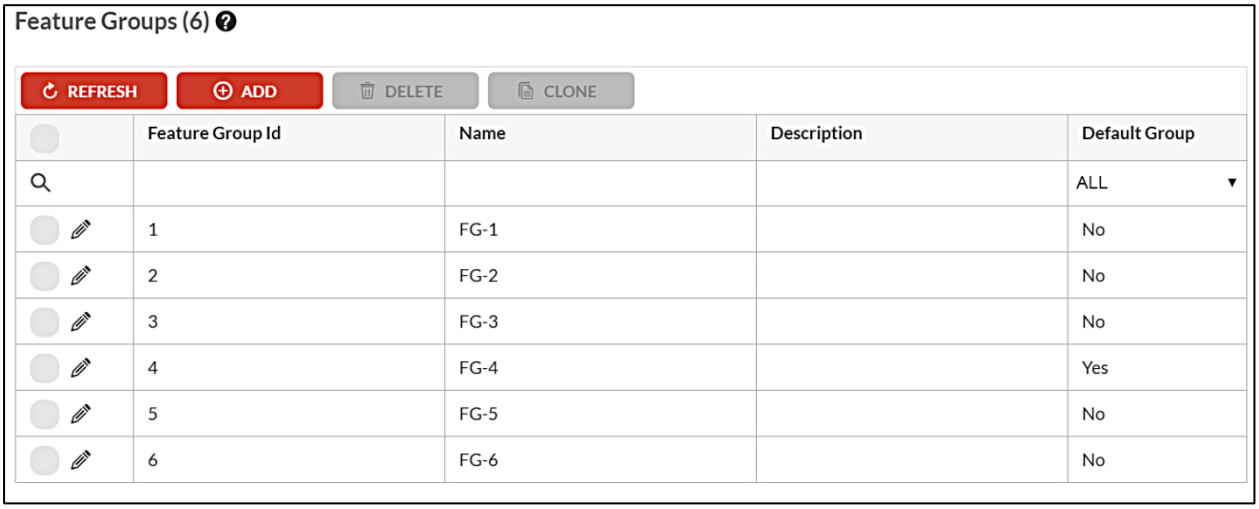
- Feature Group
- Scaled Configuration Profiles Entries
- UI Enhancements
- Support for BLE Services
- Support for CAPWAP
- HOTSPOT 2.0 Support
- Support for WIPS

# Feature Group

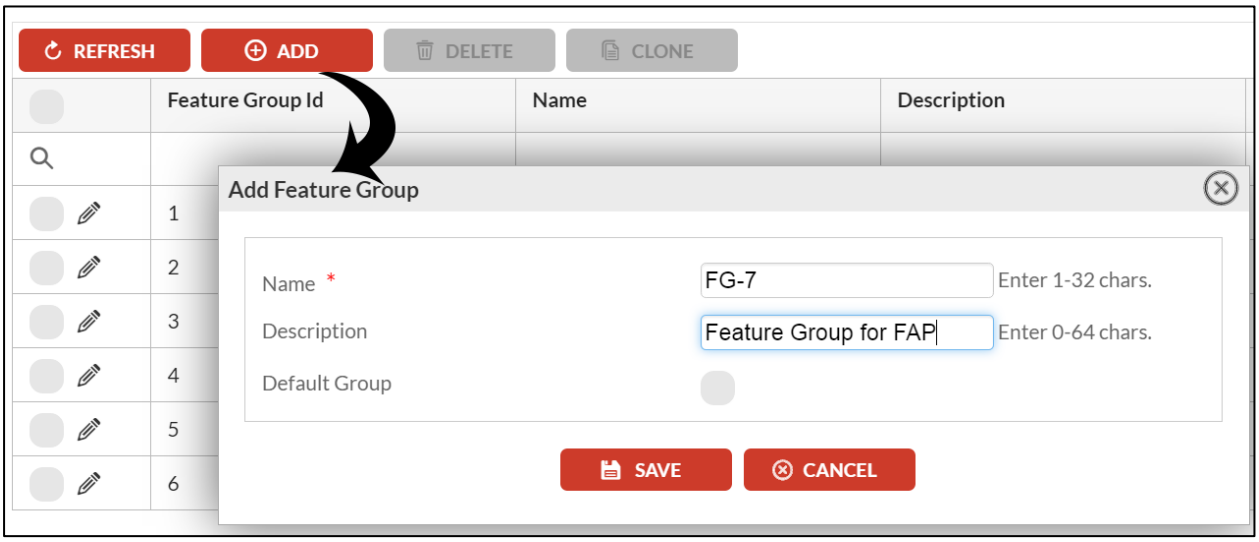
Feature group makes it easier to deploy and manage configuration. Until now, you would apply single configuration profile/settings to an AP or an AP group. Using feature groups, you can apply a set of configurations, like the ESS Profile, DPI Policies, Port-Profile, ARRP, and Radio interface settings to one or more APs or AP Groups.

## Creating a Feature Group

1. Navigate to Configuration > System Config > Feature Group.



2. In the feature group, click the ADD button. In the Add Feature Group pop-up, enter the following:




   a. **Name**: A name for this feature group. Special characters and spaces are not allowed.
   b. **Description**: Enter additional information describing this feature group
   c. **Default Group**: Select this option to set this group as a default group. All new APs that join then network become part of this feature group. You can have only one default group.

- You can create a maximum of 10 feature groups.
- If you have a default AP group, then the AP group takes precedence and all APs that join the controller will be associated with the default AP group

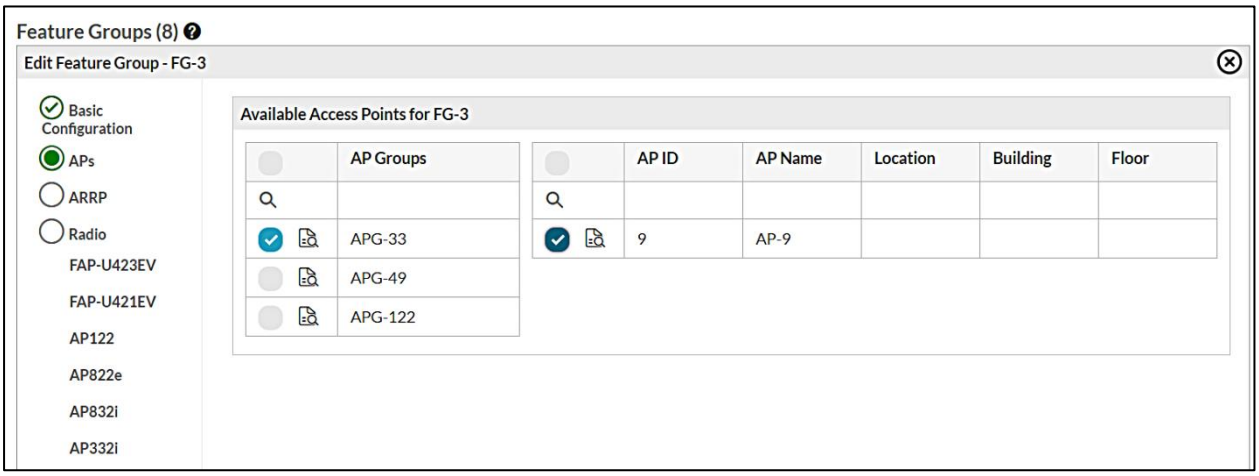
## Associate APs or AP Groups to Feature Group

You can either add an AP directly to a feature group or add an AP to an AP group and map the AP group to the feature group. An AP can be part of only one AP group or one feature group at any point of time.

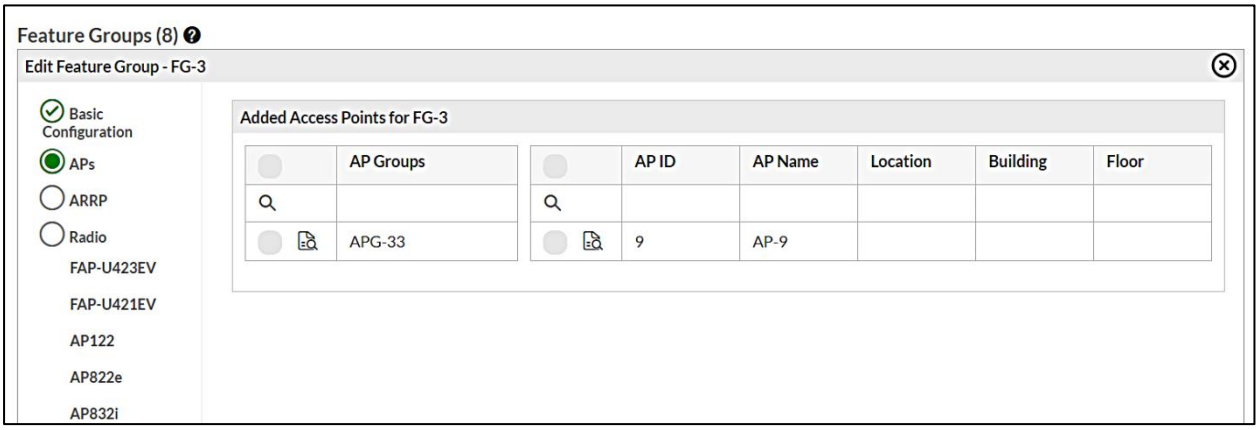
To manually add APs to a feature group, click the edit icon in the first column of the AP groups table.

1. In the Edit Feature Group section, select APs and click the Add button to view the list of APs and AP groups in your network.

2. You can select APs or AP groups by selecting the checkbox in the AP column header. To select individual APs, select the corresponding checkbox.




3. Click SAVE to add APs and AP groups to the feature group. This page refreshes to display the list of APs added to the group.



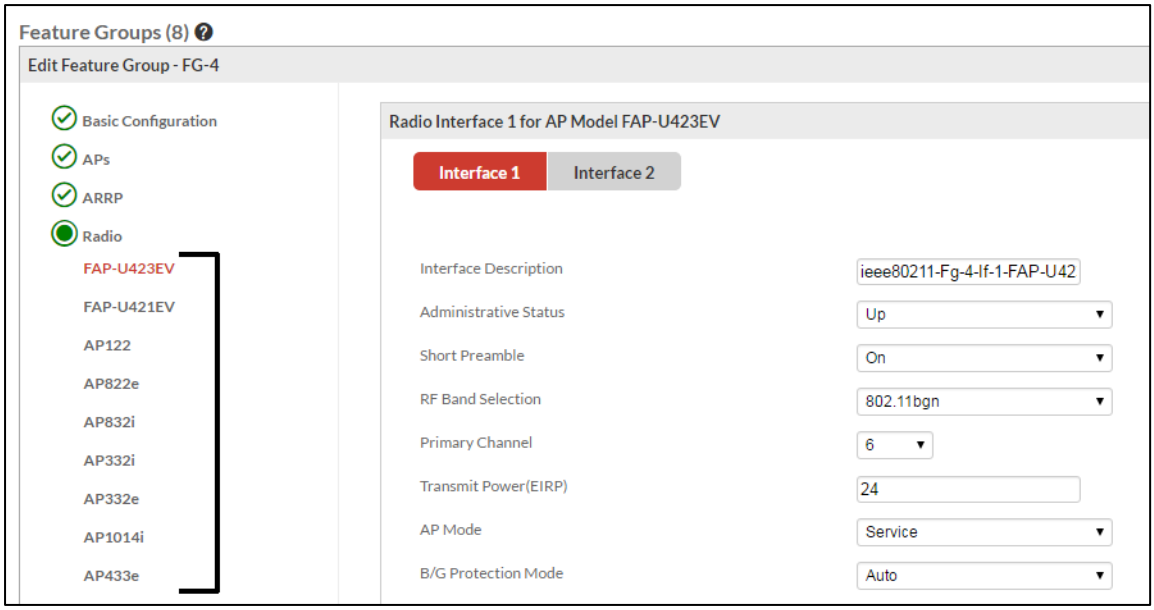

# Adding Feature Group Profiles

## ARRP

ARRP profiles are local to the group. Select this option to add ARRP configurations. It is recommended that you enable ARRP only after adding APs and AP groups to the feature group.

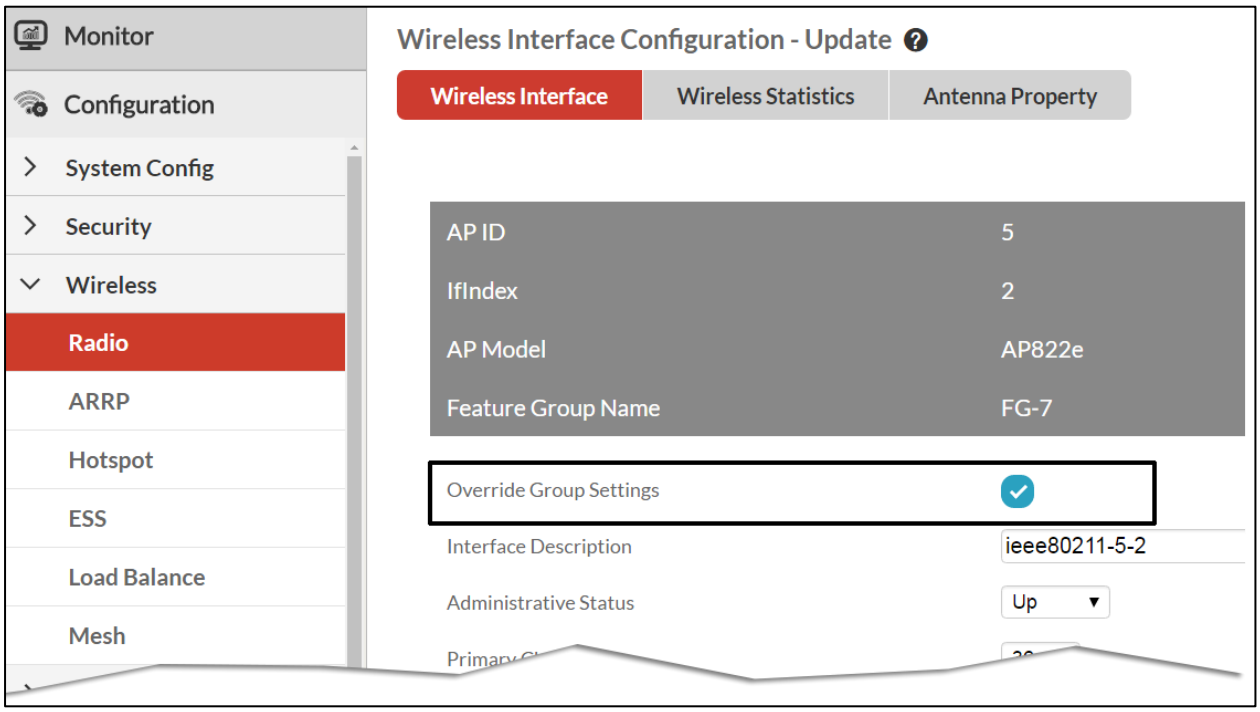
## Radio

Select this option to specify the radio interface and its antenna settings. This option lists all APs by model name.  For example, if you have 100 AP 832, you will see one entry for AP832 under the Radio option. Any changes made to the interface or antenna settings will result in the reboot of that AP model.

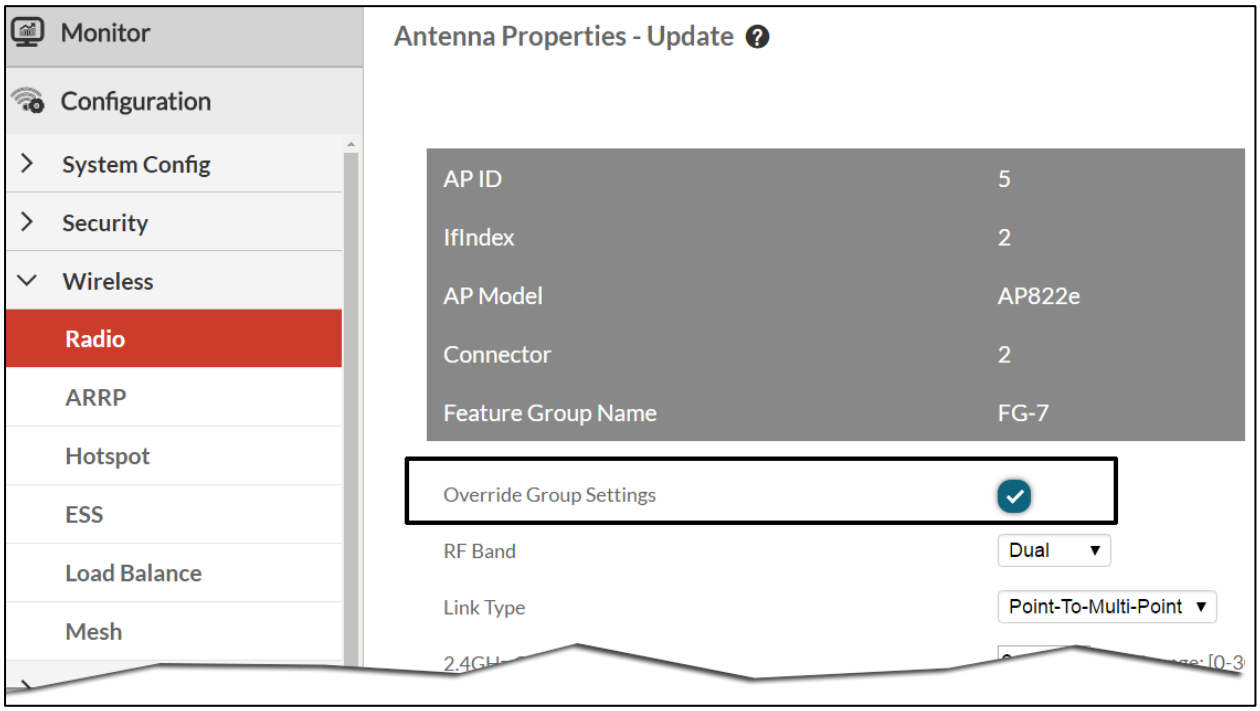



To restrict feature group related radio or antenna property changes for specific APs in a feature group, enable the *Override Group Settings* option in ***Wireless Interface*** and ***Antenna property*** sections in Configuration > Wireless > Radio page. This can be enabled per interface of an AP.

## Wireless Interface



### Antenna Property




### ESS

Select this option to select and associate ESS profiles at the interface level. An ESS profile can be mapped to more than one feature group.

### Port Profiles

Select port profile to associate at the interface level. A port profile can be mapped to more than one feature group.

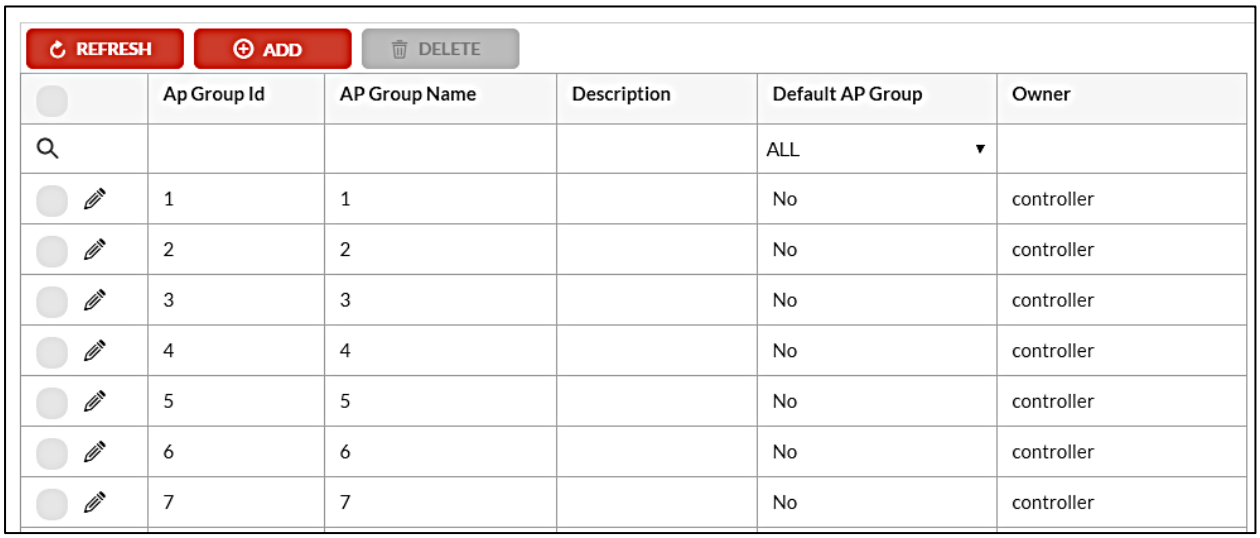
### DPI Policies

Allows you to create DPI policies for the feature group. Each feature group can contain a maximum of 25 DPI policies. DPI policies are local to group but it must be enabled at Configuration > Access Control > Application > Settings (tab). The global rules and limitations (DSCP and bandwidth limitation) for DPI policies are applicable to policies created for a feature group.

## AP Groups

Create AP groups with list of APs associated in this controller. The AP groups can be mapped to feature groups to easily deploy configurations to the associated APs.

You can create a maximum 128 AP groups. The maximum number of APs in an AP group is same as the maximum supported by the controller.



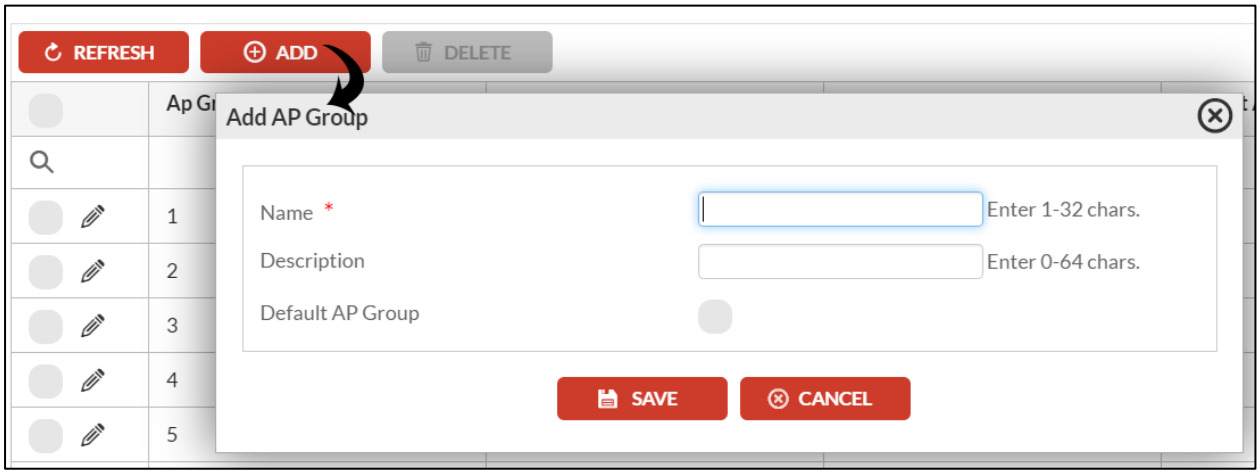

The default page, lists available AP groups with the following details about each of the AP groups:

- AP Group ID: A unique number associated with the AP group.
- AP Group Name: Name of the AP group.
- Description: Descriptive text about the AP group.
- Default AP Group: Specifies if an AP group is set as default. If set as default, all APs that join the controller will be associated with this AP group. You can have only one default group.

The default AP group takes precedence even if you have a default feature group.

## Creating an AP Group

Click the Add button and specify name (special characters and spaces cannot be used), description and also select if this group is the default AP group.

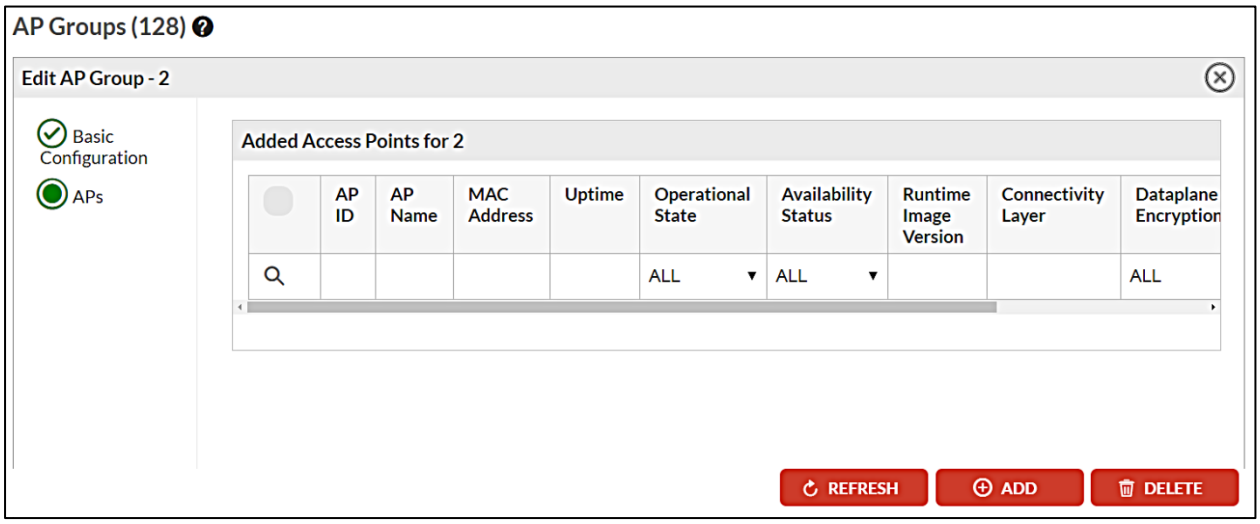



Click **SAVE** to complete this step.

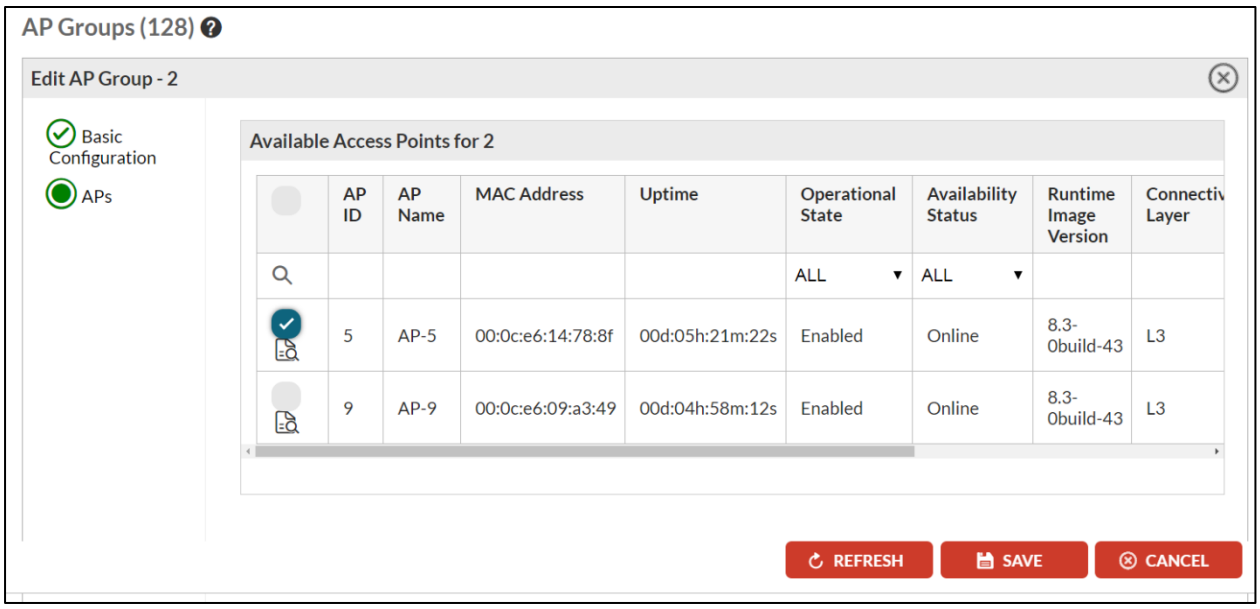
## Adding APs to the AP Group

Click the edit icon to view the group details. The Basic Configuration option is available to make changes to details like the group name, description and default group status.

Click the APs option to start adding APs to the AP group. By default this page shows the list of APs added to the AP group.




To add APs, click the ADD button to see the list of available APs.




Select one or more APs and click the SAVE button.

# Scaled Configuration Profiles Entries

Scale limits for profiles in FortiWLC-1000D and FortiWLC-3000D have increased. The following tables list the new limits:

| Profile | Limits (in 8.3.0) |
|---|---|
| Security | 128 |
| Radius | 64 |
| Captive Portal | 16 |
| Guest Users | 3000 |
| MAC Filtering (ACL Allow Access List) | 3000 |
| MAC Filtering (ACL Deny Access List) | 3000 |
| ESS | Max 256 in controller<br>Max 64 per AP<br>Max 16 per Radio |
| Backup ESSID | 16 |
| VLAN + GRE | 1024 |
| AP Groups | 128 |

# UI Enhancements

FortiWLC (SD) WebUI and FortiWLM WebUI are aligned to provide similar user experience across both these products. Notable changes include the grouping of categories in the left side.

- Only the options specific to a group are displayed.
- The operation buttons for any table data are placed above the table.
- The left pane primary navigation is aligned to other Fortinet products.
- Large table data now have pagination.

# Support for BLE Services

The following BLE services are now available in FortiWLC-SD.

## Location Services

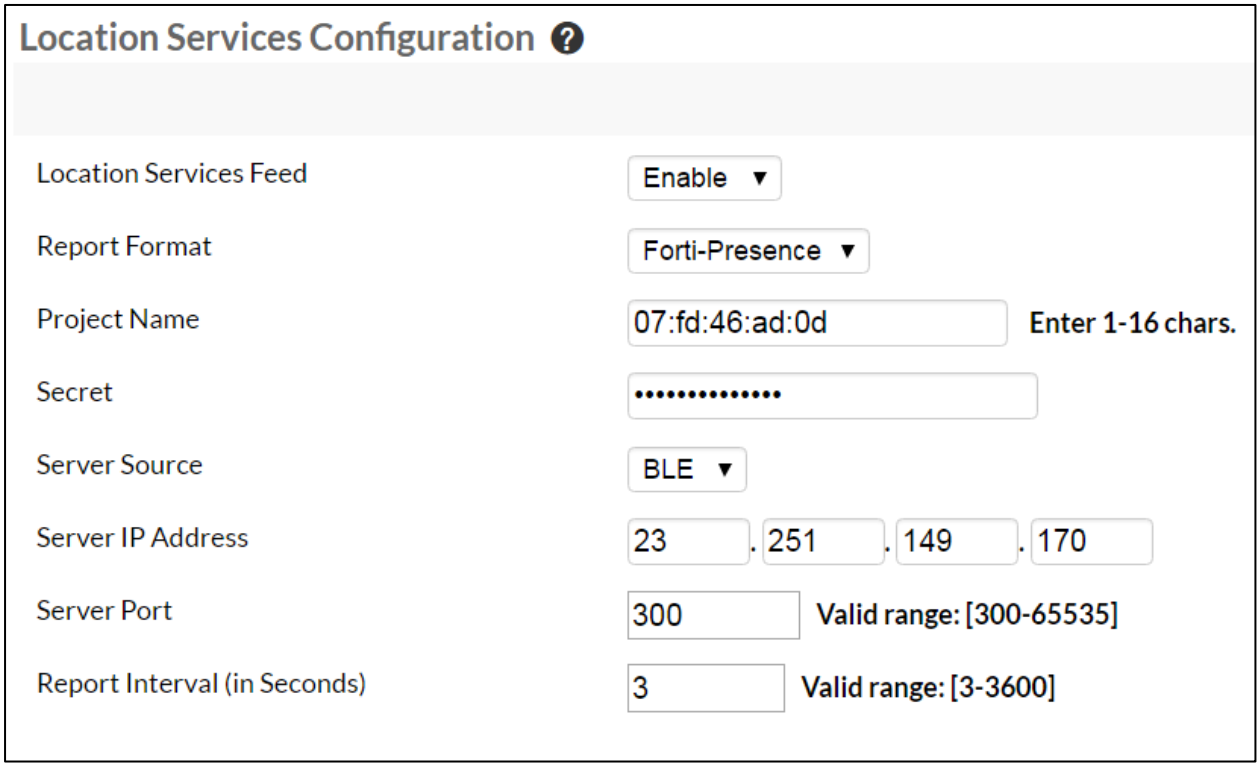
Location services are enhanced to detect and locate BLE devices. The BLE services are available by default in FortiAP-U421EV and FortiAP-U423EV. For other non-wave2 APs, you will need Bluetooth adapters (For example: Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Bluetooth Dongle, Iogear Bluetooth 4.0 USB Micro Adapter GBU521). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.

Access points must be connected to 802.3at power supply.

### Configuring Location Services for BLE

Navigate to Configuration > Devices > Location Services.

Enter the following to set up your controller to send BLE date to your location server:



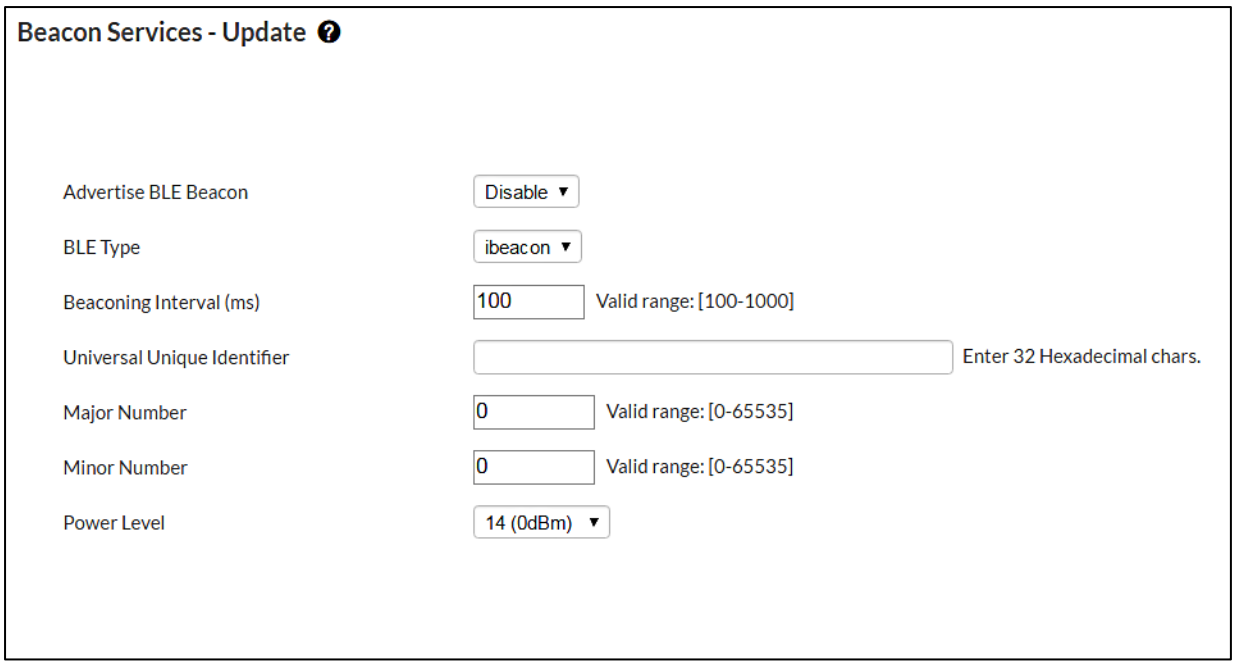

1. Enable **Location Services Feed**.
2. Select **Report Format**.
    a. Use the ***Forti-Presence*** option to send data supported by the Forti-Presence server. You will be required to set up and configure the Forti-Presence server to process the BLE data received from the controller.
    b. Use the ***Legacy*** option to send data to any other 3rd party location server.
3. Enter a name for this location service, **Project Name**.
4. Specify the **Secret** key for this location service.
5. Select *BLE* in **Server Source** to send Bluetooth data. Select both to send WiFi and Bluetooth data.
6. Enter the IP address of the location server. You can location server must have capabilities to parse and display BLE data received from the FortiWLC.
7. Enter the Port of the location server.
8. Enter the time interval at which the data is sent to the location server.

## Beacon Services

With this release of FortiWLC-SD, 11ac APs can now send iBeacons that will help advertise hyperlocal content to users in context to their location.

**Supported APs**: AP122, AP822, AP832 (the APs will require a Bluetooth dongle)

To use the beacon services, navigate to Configuration > Security > Beacon Services and click the **Add** button to enter the following details:




- Enable Advertise BLE Beacon to start the services
- Select ibeacon from BLE type
- Select the time interval at which the beacons are sent
- Enter a UUID that is specific to your network and also specify the respective Major Number and Minor Number.
- Select Power Level

# Support for CAPWAP

FortiWLC-SD 8.3.0 now supports Control and Provisioning of Wireless Access Points (CAPWAP) protocol to allow Fortinet access points to discover Fortinet WLAN controllers. In addition to controller discovery, APs can send keep-alive packets to controllers via CAPWAP.

This is a partial implementation of the CAPWAP protocol that is limited to controller discovery, keep-alive packets (echo request and response), AP image upgrade, and tunnelled client data packets between AP and controller.

## Legacy AP Discovery Process

There are three types of access point discovery:

- Layer 2 only—Access point is in the same subnet as controller.
- Layer 2 preferred—Access point sends broadcasts to find the controller by trying Layer 2 discovery first. If the access point gets no response, it tries Layer 3 discovery.
- Layer 3 preferred—Access point sends discovery message to the controller by trying Layer 3 discovery first. If the access point gets no response, it tries Layer 2 discovery.
- Layer 3 only—Access point sends discovery message to the controller by trying Layer 3 only.

For Layer 2 and Layer 3 discovery, the access point cycles between Layer 2, Layer 3, and Mesh (if mesh is enabled) until it finds the controller.

An access point obtains its own IP address from DHCP (the default method), or you can assign a static IP address. After the access point has an IP address, it must find a controller's IP address. By default, when using Layer 3 discovery, the access point obtains the controller's IP address by using DNS and querying for hostname.

After the access point obtains the controller IP address, it sends discovery messages using UDP port 9292. After the controller acknowledges the messages, a link is formed between the AP and the controller.

# CAPWAP and Legacy Reference

## Port Requirements

| Activity | CAPWAP UDP Ports | L3 UDP Ports | Ethertype (L2) |
|---|---|---|---|
| Discovery | 5246 | 9292 | 0x4003 |
| Configuration and Keep-Alive | 5246 | 5000 | 0x4001 |
| Data Flow | 5247 | 9393 | 0x4000 |

If Firewalls/packet filtering devices are used in your network, ensure the ports mentioned in this table are allowed.

# Controller and AP Communication Ports

| AP firmware version | Discovery Mode | Discovery Port / Ethertype | keep-alive ports / Ethertype | Configuration ports/Ethertype | Data Flow Ports / Ethertype | Notes |
|---|---|---|---|---|---|---|
| Pre-8.3 (*8.2, 8.1, 8.0, 7.0, etc.,*) | L2 | 0x4003 | 0x4001 | 0x4001 | 0x4000 | |
| | L3 | 9292 | 5000 | 5000 | 9393 | After upgrade, UDP 5246 and 5247 is used for future discovery process and data flow respectively. |
| 8.3.0 | L2 | 0x4003 | 0x4001 | 0x4001 | 0x4000 | |
| | L3 | 5246 | 5246 | 5000 | 5247 | |

# CAPWAP Discovery

The CAPWAP protocol requires the UDP ports 5246 and 5247 to exchange control and data packets respectively

### Discovery Sequence

The CAPWAP discovery supports the following sequence on port UDP 5246:

1. Unicast Options
    a. Controller IP address: AP sends discovery request to a controller based on the configured IP address in the AP.
    b. DHCP Option 138: AP sends discover request to the controller configured with DHCP option 138. Alternatively, option 43 is also available for discovering controller.
    *c. DNS: AP sends discovery request based on the DNS resolution of -* ***_capwap-control._udp.example.com***

### Discovery Process

1. In L3 discovery mode, the AP sends discovery request on both port 5246 and port 9292 to the controller.
2. If the controller is already upgraded to the 8.3 release, it sends response on port 5246 to complete the AP association.
3. Further the keep-alive and image upgrade message exchange happens on port 5246.
4. Tunnelled client data are sent to controller on port 5247.

## Upgrading from Pre-8.3 Release

### Using the `upgrade controller` command with auto-ap-upgrade ON

1. The controller is upgraded to 8.3 and will now listen on port 5246 and 9292 for discovery request from access points. During the controller upgrade process, the pre-8.3 access points will continue re-discovery of the controller using the legacy method.
    a. Once the controller is upgraded, the pre-8.3 APs will associate with the controller using the legacy method.
2. Now, the access points begin the upgrade process. After the upgrade is complete, the access points will send discovery request on port 5246 and port 9292. The controller that is already upgraded to 8.3 will respond on port 5246 to complete AP association.

### Using the `upgrade system` command

1. The APs are upgraded first to the 8.3 release. After upgrade the APs will send discovery request using a method sequence as mentioned in the Discovery Sequence section.
2. The controller is upgraded to 8.3 after the APs are upgraded. The 8.3 controller will respond to AP discovery request.

### Post Upgrade

Ensure that UDP 5000 is open after the upgrade is complete.

### Downgrading

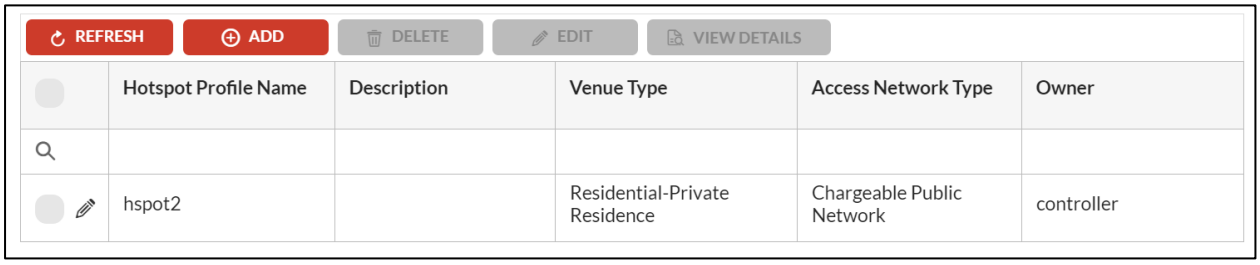
When downgraded to a previous release, the discovery mechanism will switch back to the legacy discovery process. However, we recommend that you open the CAPWAP UDP ports, Kcom (L3) UDP ports, and Ethertypes.

# HOTSPOT 2.0 Support

Supported only on Wave-2 Access Points (FAP-U423EV and FAP-U422EV).

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between Wi-Fi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.

The Hotspot Profiles can be created from the Configuration > Wireless > Hotspot. The following table provides the details of the HotSpot Profile.



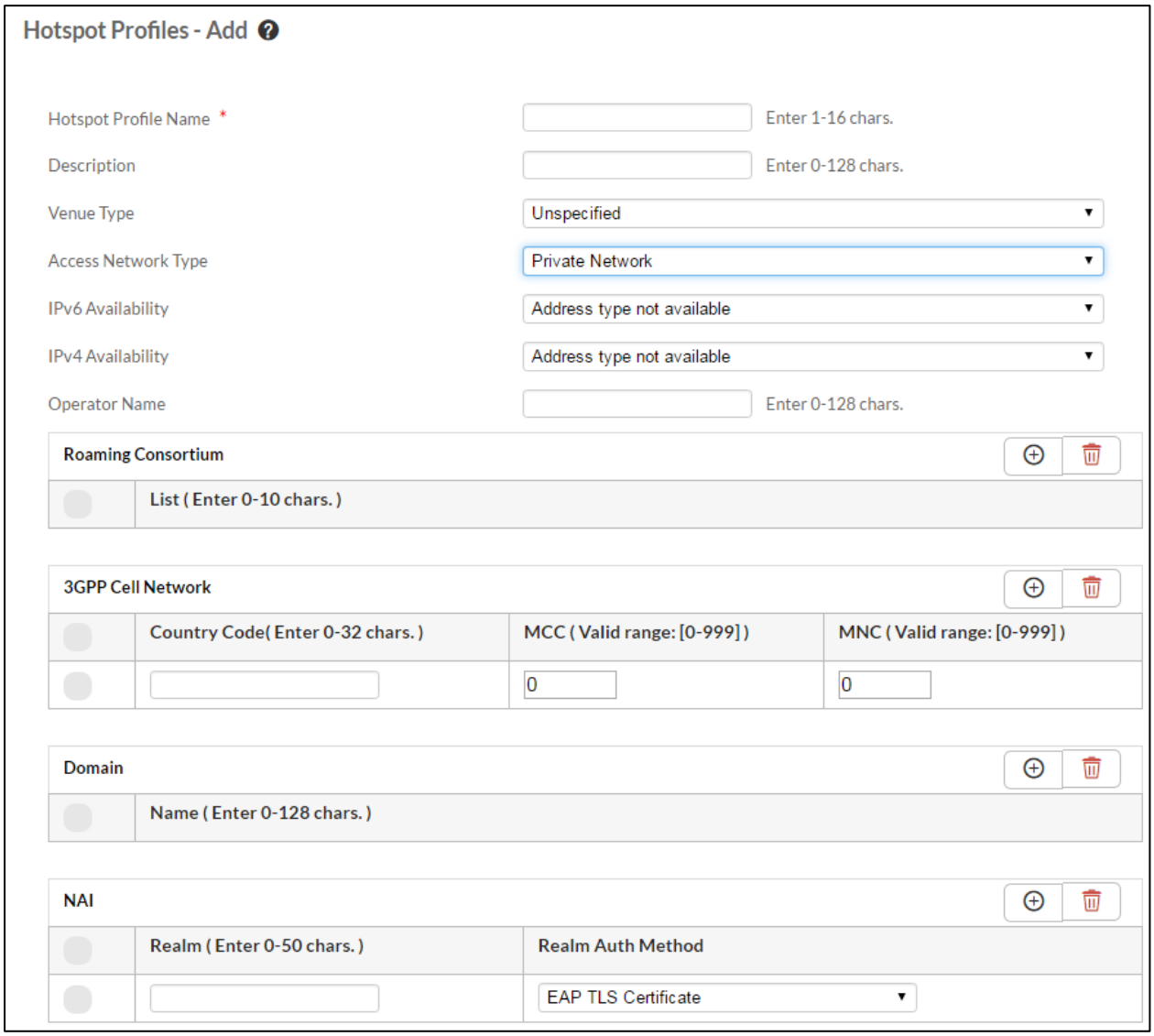

| Field | Description |
|---|---|
| Hotspot Profile Name | The name of the Hotspot profile |
| Description | Description provided for the Hotspot profile |
| Venue Type | The venue type field in the information element provides additional information about the group and type of hotspot venue. The hotspot operator shall configure the Passpoint AP with one of the venue group description values, such as "business" or "educational" from the drop down box. |
| Operator Name | The hotspot operator, at its discretion, can configure the information in the AP to describe the venue in which the hotspot is located. |
| Access Network Type | The access network type field is automatically included in the IEEE 802.11u interworking element present in beacon and probe response frames in PAPs. Mobile devices can use this information when selecting a hotspot. The access network type are as follows:<br>• Private Network<br>• Private Network with Guess Access<br>• Chargeable Public Network<br>• Free Public Network<br>• Personal Device Network |

| Field | Description |
|---|---|
| | • Emergency Services Only Network<br>• Test or Experimental Network<br>• Wildcard Network |
| Owner | Owner of the Hotspot profile |

## Add Hotspot Profile

To add the Hotspot profile, perform the following steps:

1. Select Configuration > Wireless > Hotspot.
2. Click Add.




| Field | Description |
|---|---|
| Hotspot Profile Name | Enter Hotspot profile name; this is a required field and the valid range 1-16 characters. |
| Description | Enter the description provided for the Hotspot profile |
| Venue Type | Select the venue type from the drop-down list. The venue type field in the information element provides additional information about the group and |

| Field | Description |
|---|---|
| | type of hotspot venue. The hotspot operator shall configure the Passpoint AP with one of the venue group description values, such as "business" or "educational" from the drop down box. The default selection is displayed as Unspecified. |
| Access Network Type | Select the Access Network type from the drop down list. The access network type field is automatically included in the IEEE 802.11u interworking element present in beacon and probe response frames in PAPs. Mobile devices can use this information when selecting a hotspot. The default selection is displayed as Private Network and the options are as follows:<br>• Private Network<br>• Private Network with Guess Access<br>• Chargeable Public Network<br>• Free Public Network<br>• Personal Device Network<br>• Emergency Services Only Network<br>• Test or Experimental Network<br>• Wildcard Network |
| IPv6 Availability | Select the IPv6 availability from the drop-down list. The default selection is Address type not available and the options are as follows:<br>• Address type available<br>• Address type not available<br>• Availability of the Address type not known |
| IPv4 Availability | Select the IPv4 availability from the drop-down list. The default selection is Address type not available and the options are as follows:<br>• Address type available<br>• Address type not available<br>• Availability of the Address type not known<br>• Port-restricted IPv4 address available<br>• Single NATed private IPv4 address available<br>• Double NATed private IPv4 address available<br>• Port-restricted IPv4 address and single NATed IPv4 address available<br>• Port-restricted IPv4 address and double NATed IPv4 address available |
| Operator Name | Enter the operator name for the Hotspot profile. The valid range is 0-100 characters. |
| Roaming Consortium | Enter the roaming ORG ID for the Hotspot profile. The valid range is 0-10 characters. |
| 3GPP Cell Network | • Enter Country Code.<br>• Enter the 3GPP cell network MCC; the default value displayed is 0 and the valid range is 0-999.<br>• Enter the 3GPP cell network MNC; the default value displayed is 0 and the valid range is 0-999. |
| Domain Name | Enter the domain name for the Hotspot profile. The valid range is 0-128 characters. |
| NAI | NIA Realm: Enter the NAI realm. Realms that can authenticate a mobile device's username/password or certificate credential shall be added to this list. The valid range is 0-50 characters.<br>Realm Auth Method: Select the NAI realm authentication method from the |

| Field | Description |
|---|---|
| | drop-down list. The default selection is EAP TLS Certificate and the options are as follows:<br>• EAP TLS Certificate<br>• EAP TLS MSCHAPv2 Username/Password<br>• EAP SIM<br>• EAP AKA<br>• EAP AKA` |

# Support for WIPS

WIPS (Wireless Intrusion Prevention System) management options are available in FortiWLC-SD configuration. You can access WIPS configurations options from **Configuration** > **WIPS** > **WIPS Management** page.

By default WIPS services is disabled. For configuration options, refer to the WIPS online help in the FortiWLC WebUI.

# Fixed Issues

| Bug-ID | Description | Notes |
|---|---|---|
| 0383337 | Fixed issues that resulted in users getting incorrect internal CP page. | The issue was noticed in FortiWLC-SD 8.1. |
| 0393924 | Fixed controller crash issues. | |
| 0402763, 0401322 | Issues with configuring DNS and domain name via the initial set up wizard is fixed. | The issue affected FortiWLC-SD 7.0 MR release. |
| 0402755 | Fixed configuration loss issues. | The issue occurred when upgrading from 8.1-3MR to 8.1-3-2. |
| 0377349 | Fixed authentication issues with Motorola MC3000 devices | The issue was seen in FortiWLC-SD 8.1 |
| 0383560 | Fixed guest authentication issues via captive portal. | - |
| 0381029 | Fixed restart issues with SecurityMM module. | The issue was noticed in FortiWLC-SD 8.1. |
| 0378696 | Fixed controller crash issues. | The issue was noticed in FortiWLC-SD 8.1-2-0. |
| 0377362 | Fixed captive authentication failure issues. | The issue was noticed in FortiWLC-SD 8.1 |
| 0353992, 0377362 | Fixed external captive portal authentication failure issues. | The issue was noticed in FortiWLC- SD 8.0 |
| 0380116 | Fixed AP822 crash issues. | The issues occurred in AP822 running 8.1.2 when a change to an ESS profile was made. |
| 0382927 | Fixed issue that resulted in clients not getting IP from SSIDs that had GRE tunnel. | The issue was seen in FortiWLC-8.1.2.0 |
| 0397318 | Tx freeze issues after 99 days of uptime has been fixed. | The issue was noticed in AP832 running FortiWLC-SD 8.1 |
| 0369867, | Fixed AP reboot issues. | This was occasionally noticed with |

| Bug-ID | Description | Notes |
|---|---|---|
| 0386327, 0387936 | | AP832 after it was upgraded to 8.0-SR1-2 from 8.0-5-0. |
| 0391047 | Fixed client connectivity issues. | This issue was noticed in FortiWLC-SD 8.1 with clients having Broadcom chipset BCM943228Z. |
| 0407596 | CP Profile redirection is fixed to redirect to HTTP link. | The issue was seen in FortiWLC-SD 8.1-3-MR |
| 0395009 | Fixed client disconnection issues. | The issue was seen in FortiWLC-SD 8.1-3MR. |
| 0412302 | Fixed location services issues with WiFi clients. | The issue affected FAP U423EV running 8.3.0 |
| 413814, 0375945 | Fixed vulnerability issues.related to undocumented account and escalation of privilege. | The issue affected SD 8.0-6-0, 8.3.0 |

## Common Vulnerabilities and Exposures

FortiWLC 8.3.0 is no longer vulnerable to the following CVE-Reference:

- 2017-3134
- Visit https://fortiguard.com/psirt for more information

# Known Issues & Limitations

| Bug ID | Description |
|---|---|
| 0408382 | Continuous RTS frames resulting in degraded performance & ping loss. Issue affects FAP-U42xx. |
| 0408381, 408380 | Transmission of incorrect frames resulting in degraded performance & ping loss. Issue affects FAP-U42xx. |
| 408379 | 11AC mobile clients are unable to connect and display *IP Configuration Failure* message. Issue affects clients connected to FAP-U42xx. |
| 408163 | Client are unable to retain the same IPv6 address after roaming to a different controller in the same roaming domain. |
| 408158 | Issues with *hostapd* process result in client disconnections. |
| 408117 | Rate adaptation is not working as expected for FAP-U423, resulting in poor throughput. |
| 407928 | In a dual Ethernet configuration, if the secondary interface is dynamic, the system is non-operational. |
| 407923 | Mesh APs do not get into *Enabled-Online* state and remain *Disabled-Online* state. |
| 407878 | APs reboot before completing link probe. |
| 407650 | Poor throughput and ping loss is noticed on some clients with Marvel chips. |
| 407395 | Same IP is simultaneously assigned to both, a wireless & a wired station. |
| 407135, 402726 | Increased memory usage results in *wncagent* process restart. |
| 406540 | 11AC clients experience poor network performance after roaming.<br>Issue affects clients connected to FAP-U42xx. |
| 406525 | AP832 gets into Disable-Offline state and the console access is lost. |
| 404699 | Co-ordinator process crash is noticed in FortiWLC-1000D in a scale setup. |

| Bug ID | Description |
|---|---|
| 402896 | Station throughput graph is not updated. Issue affects FortiWLC-1000D in a scale setup with heavy traffic. |
| 400671 | Stuck AP radios resulting in client disconnections. |
| 398600 | Unable to create/enable/disable packet capture profile when rogue AP detection is ON. |
| 390672 | In case of primary partition corruption, controller does not auto-reboot into secondary partition. |
| 0409090 | Device fingerprint name for all versions of Android Jellybean are not available. |
| 0409089 | Application visibility stops working if an ESSID that is part of a feature group is added to a global DPI policy. |
| 0409092 | WebUI does not display the correct updated hostname. |
| 0410454 | Mac book Pro asks for "username" and "password" even for "PSK" profile if 11r is enabled. |
| 0413369 | If the disk space is full during operation, it may result in stale entries of disassociated stations. |
| 0402749 | Usernames with special characters are processed as escape sequence. For example, a username somename****tempname will be processed as somename**<space>**empname. |
| 0410009 | Fingerprint edit option in the WebUI does not work as expected. |
| 0402944 | FWC3000D does not support jumbo frames. |
| 0410004 | The output of ***sh interfaces Ethernet ap*** and ***sh interfaces Dot11Radio statistics*** are not filtered correctly. |
| 0410873 | The hostapd process crash results in client re-authentication. |
| 0411544 | The ***sh interfaces Dot11Radio statistics*** command output does not display AP name |
| 0412640 | The ***reload-management*** command clears AP ID's & AP Names from the ***sh station*** command output. |
| 0413369 | The ***show station all*** command lists stations that disassociated or aged out. |
| 0413803 | The RF Band Field is listed as "Unknown" in the ***sh station*** command output. |
| 0413804 | Mismatch in station count when cursor is hovered on any particular SSID in the Stations by SSID pie chart, |
| 0413811 | There are known issues that cause hostapd process crash resulting in minor client disconnections. |
| 0414579 | Continuously executing the **cat /proc/meru/kcomm/mailboxes** results in loop state. |
| 0401680 | There are known issues that cause redis-server process restart which results in non-existent stations being listed in the station count. |
| 0381027, 0353992, 0377362 | In case of multiple external Captive Portal profiles, and when wireless clients toggle between these profiles, intermittent authentication failures are seen. |

# END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

## Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service